UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,773	12/09/2003	Akashi Satoh	JP920020207US1	4832

48813 7590 09/19/2008

LAW OFFICE OF IDO TUCHMAN (YOR)
ECM #72212
PO Box 4668
New York, NY 10163-4668

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
09/19/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

pair@tuchmanlaw.com
idotuchman@gmail.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/730,773
Filing Date: December 09, 2003
Appellant(s): SATOH ET AL.

Ido touchman
Reg. No. 45,924
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 01/02/08.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20010056541 A1	Matsuzaki et al.	12-2001
5,604,800	Johnson et al.	2-1997
7,062,652 B2	Hirota et al.	6-2006
EP 0 911 738 A2	Jackson et al.	10-1998

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1, 2, 5, 6, 13-23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki et al. US 2001/0056541 A1 (hereinafter Matsuzaki) in view of Johnson et al. US 5,604,800 (hereinafter Johnson).

As per claim 1, Matsuzaki teaches a data storage device for an information processing device, the data storage device comprising:

an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152];

a recording medium for recording the data and the personal identification information encrypted by the encryption circuit (i.e., writing the encrypted password and encrypted file key as a file) [paragraphs 0141 and 0152]; and

a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium (i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]). Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson

teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

As per claim 5, Matsuzaki teaches a data storage device for an information processing device, the data storage device comprising:

an encryption circuit for encrypting desired data by use of a first encryption key (i.e., encrypting plaintext file using file key) and for encrypting the first encryption key (i.e., encrypting file key using read key) and personal identification information by use of a second encryption key (i.e., encrypting password using read key) [paragraphs 0141, 0147, 0148 and 0152]

a recording medium for recording the data encrypted by use of the first encryption key, the first encryption key encrypted by use of the second encryption key, and the personal identification information encrypted by use of the second key (i.e., writing the encrypted data, encrypted password and encrypted file key as a file) [paragraphs 0141, 0148 and 0152]; and

a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium (i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]). Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious

to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

As per claims 13 and 14, Matsuzaki teaches an information processing device comprising:

an operation control unit for executing various operation processing [figure 10, File management apparatus]; and

a data storage device for storing data to be processed by the operation control unit [figure 10, File management apparatus],

wherein the data storage device includes an encryption function for encrypting desired data by use of a data encryption key (i.e., encrypting plaintext file using file key) and for encrypting personal identification information by use of an verification encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152], and

the data storage device executes user verification by use of the encrypted personal identification information (i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]). Matsuzaki is silent on the device wherein the verification encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

As per claims 17 and 22, Matsuzaki teaches a data processing method for a data storage device for executing data writing and reading in and out of a recording medium of a data storage device, the data processing method for a data storage device comprising the steps of:

encrypting personal identification information by use of an encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data (i.e., encrypting password using read key and storing the encrypted password) [paragraphs 0141 and 0152];

executing user verification based on the verification data recorded in the recording medium(i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]); and

executing any of encrypting write data transmitted from a host system by use of the encryption key and thereby recording the encrypted write data in the recording medium (i.e., encrypting file key by using read key) [paragraph 0152], and, decrypting the data read out of the recording medium by use of the encryption key and thereby transmitting the decrypted data to the host system (i.e., decrypting the encrypted file key using the read key) [paragraph 0161]. Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

As per claims 19 and 23, Matsuzaki teaches a data processing method for a data storage device for executing data writing and reading in and out of a recording medium of a data storage device, the data processing method for a data storage device comprising the steps of:

encrypting a personal identification information by use of a verification encryption key and recording the encrypted personal identification information in the recording medium as verification data (i.e., encrypting password using read key and storing the encrypted password) [paragraphs 0141 and 0152], and further encrypting a data encryption key by use of the verification encryption key (i.e., encrypting file key using read key) and thereby recording the encrypted data encryption key in the recording medium [paragraphs 0141 and 0152];

executing user verification based on the verification data recorded in the recording medium (i.e., encrypting file key by using read key) [paragraph 0152], and, decrypting the data read out of the recording medium by use of the encryption key and thereby transmitting the decrypted data to the host system (i.e., decrypting the encrypted file key using the read key) [paragraph 0161];

decrypting the data encryption key recorded in the recording medium by use of the verification encryption key (i.e., decrypting file key using read key) [paragraph 0161]; and

executing any of encrypting write data transmitted from a host system by use of the decrypted data encryption key and thereby recording the encrypted write data in the recording medium (i.e., encrypting data using file key), and decrypting the data read out of the recording medium by use of the data encryption key (i.e., decrypting data using file key) and thereby transmitting the decrypted data to the host system [paragraphs 0147, 0148 and 0164]. Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art,

which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.

As per claims 2, 15 and 16, Matsuzaki further teaches the device wherein the encryption circuit encrypts the encryption key by use of a different encryption key, and the recording medium records the encryption key encrypted by use of the different encryption key [paragraphs 0148- 0152].

As per claim 6, Matsuzaki further teaches the device wherein the encryption circuit decrypts the encrypted first encryption key being read out of the recording medium by use of the second encryption key, and executes any of encryption and decryption of the desired data by use of the decrypted first encryption key [paragraphs 0161-0164],

As per claim 18, Matsuzaki further teaches the device further comprising the steps of: encrypting the encryption key by use of a different encryption key and thereby recording the encrypted encryption key in the recording medium [paragraphs 0148-0152]; and

decrypting the encrypted encryption key by use of the different encryption key and thereby decrypting the data read out of the recording medium by use of the decrypted encryption key [paragraphs 0161-0164].

As per claim 20, Matsuzaki further teaches the device further comprising the step of: decrypting the encrypted data encryption key recorded in the recording medium along with a change in the personal identification information by use of the verification encryption key created out of the personal identification information prior to the change, and then encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change and thereby storing the data encryption key in the recording medium [paragraphs 0192-0199].

As per claim 21, Matsuzaki further teaches the device further comprising the step of: decrypting the encrypted data encryption key recorded in the recording medium upon disabling encryption of the data recorded in the recording medium by use of the verification encryption key created out of the personal identification information prior to a change and thereby storing the decrypted data encryption key in the recording medium [paragraphs 0192-0199].

As per claim 25, Matsuzaki further teaches for executing user verification by use of the encrypted personal identification information stored in the recording medium (i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]). Further Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65].

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki US 2001/0056541 A1 in view of Johnson US 5,604,800 and further in view of Hirota et al. US 7,062,652 B1 (hereinafter Hirota).

As per claim 3, the combination of Matsuzaki and Johnson teaches the claimed invention as described above. However, the combination of Matsuzaki and Johnson does not explicitly teach the device, wherein the recording medium includes a special storage area which is inaccessible in normal use, and the recording medium records the encryption key in the special storage area. In the same field of endeavor, Hirota teaches a recording medium includes a special storage area which is inaccessible in normal use, and the recording medium records the encryption key in the special storage area [see for example, column 12, lines 49-54 and column 10, lines 22-36]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Hirota within the combination of the Matsuzaki and Johnson thereby protecting access to secure data and further enhancing security of the system.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki US 2001/0056541 A1 in view of Johnson US 5,604,800 and further in view of Jackson EP 0 911 738 A2

As per claim 4, the combination of Matsuzaki and Johnson teaches the claimed invention as indicated above. Furthermore, Matsuzaki teaches device wherein the encryption circuit encrypts the encryption key by use of a different encryption key, and the recording medium records the encryption key encrypted by use of the different encryption key [paragraphs

0148- 0152]. The combination of Matsuzaki and Johnson does not teach a recording medium that manages the storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys. However, Jackson teaches a device wherein the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys [page 8, lines 33-47]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Jackson within the combination of Matsuzaki and Johnson in order to efficiently process encryption/decryption of data.

Claims 7-12 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson EP 0 911 738 A2 in view of Johnson et al. US 5,604,800 (hereinafter Johnson).

As per claim 7, Jackson teaches a hard disk device comprising:

a magnetic disk being a recording medium (i.e., mass storage device, such as floppy disks, magnetic taps) [column 5, lines 5-12];

a read-and-write mechanism for writing and reading data in and out of the magnetic disk [column 5, lines 12-15]; and

a control mechanism having an encryption function for encrypting data to be written in the magnetic disk and for decrypting the encrypted data to be read out of the magnetic disk (i.e., encryption/decryption of data to and from the disk) [column 5, lines 15-19], the control mechanism for controlling reading and writing the data by the reading-and-writing mechanism

[column 5, lines 12-15], wherein the control mechanism executes encryption of the data to be written in the magnetic disk for each unit of writing and reading data in and out of a storage area of the magnetic disk upon processing of writing the data in the magnetic disk [column 11, paragraphs 0041 & 0042], in response to turning on and off of the encryption mechanism (i.e., activating the encryption/decryption only in response to receipt of a valid password) [column 5, lines 19-34]; and

wherein the encryption function of the control mechanism encrypts personal identification information by use of an encryption key [page 7, paragraph 0028 and page 8, lines 21-32]. Jackson is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Jackson in order to enhance the security of the system.

As per claim 8, Jackson further teaches the device wherein the control mechanism judges as to whether the data are encrypted or not upon reading the data out of the storage medium, and further decrypts the data when the data are encrypted [page 11, paragraphs 0041-0042].

As per claim 9, Jackson further teaches the device wherein the control mechanism

decrypts the read-out data when the data read out of the recording medium are encrypted, and the control mechanism encrypts and writes the data in the recording medium when the encryption function is turned on [page 11, paragraphs 0041-0042].

As per claims 10 and 12, Jackson further teaches the device wherein the control mechanism includes an encryption function for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key [page 7, paragraph 0028 and page 8, lines 21-32] and the control mechanism executes user verification by use of the encrypted personal identification information [page 8, lines 21-32]. Jackson is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. However, such feature is old and well known in the art, which has an advantage of enhancing security of the system. For example, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Jackson in order to enhance the security of the system.

As per claim 11, Jackson further teaches the device wherein the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys [page 8, lines 33-47].

As per claim 24, Jackson further teaches the device wherein the control mechanism writes the data in the recording medium without encrypting the data when the encryption function is turned off [column 5, lines 19-34].

(10) Response to Argument

Appellant argues that Claims 1, 2, 5, 6, 13-23 and 25 are not obvious over Matsuzaki in view of Johnson and neither Matsuzaki nor Johnson express any appreciation provided by the examiner in the final office action.

Examiner would point out that a suggestion, teaching, or motivation to combine the relevant prior art teachings does not have to be found explicitly in the prior art, as the teachings, motivation, or suggestion may be implicit from the prior art, as a whole, rather than expressly stated in the references. The test for an implicit showing is what the combined teachings, knowledge of one of a whole would have suggested to those of ordinary skill in the art. In re Kahn, 441 F.3d 977, 988, 78, USPQ2d 1329, 1336 (Fed. Cir. 2006) citing In re Kotzab, 217 F.3d 1365,1370, 55 USPQ2d 1313 (Fed. Cir. 2000). See also In re Thrift, 298 F. 3d 1357, 1363, 63 USPQ2d 2002, 2008 (Fed. Cir. 2002). These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). In this case both Matsuzaki and Johnson are directed a security system, specifically encryption of data/key information using a password. Matsuzaki teaches encrypting desired data personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of

the personal identification information. Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. One of ordinary skill in the art at the time of applicant's invention could have been able to employ encryption key creation out of a given piece of personal identification as taught by Johnson and employ it within the system of Matsuzaki in order to enhance the security of the system by encrypting data and personal identification information by use of an encryption key made out of a given piece of personal identification information, thereby making it difficult to re-create the encryption key by someone having no knowledge of the personal identification information.

Claim 1

Appellant argues that, the cited portions of Matsuzaki fails to teach encrypting personal identification information and using a piece of the personal identification information as an encryption key. Appellant further argues that the cited portions of Johnson do not disclose encrypting personal identification information and creating an encryption key out of a piece of the personal identification information.

Examiner would point out that, in the present application, the term 'personal identification information' is referred as " ... personal identification information by use of an encryption key created out of a given piece of the personal identification information such as a password ..." [specification page 9, lines 7-10], therefore it is clear that the claimed created out of a given piece of the personal identification information is reasonably interpreted as a password. The personal identification information in Matsuzaki and Johnson is directed to a password and/or personal ID. Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by

use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65].

Appellant further argues that the Office action has not explained, and it is not evident, how employing the teachings of Johsnon within the system of Matsuzaki enhances the security of the system.

Examiner would point out that a suggestion, teaching, or motivation to combine the relevant prior art teachings does not have to be found explicitly in the prior art, as the teachings, motivation, or suggestion may be implicit from the prior art, as a whole, rather than expressly stated in the references. The test for an implicit showing is what the combined teachings, knowledge of one of a whole would have suggested to those of ordinary skill in the art. In re Kahn, 441 F.3d 977, 988, 78, USPQ2d 1329, 1336 (Fed. Cir. 2006) citing In re Kotzab, 217 F.3d 1365,1370, 55 USPQ2d 1313 (Fed. Cir. 2000). See also In re Thrift, 298 F. 3d 1357, 1363, 63 USPQ2d 2002, 2008 (Fed. Cir. 2002). These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). In this case both Matsuzaki and Johnson are directed a security system, specifically encryption of data/key information using a password. Matsuzaki teaches encrypting desired data personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. Johnson teaches a personal authentication device,

including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. One of ordinary skill in the art at the time of applicant's invention could have been able to employ encryption key creation out of a given piece of personal identification as taught by Johnson and employ it within the system of Matsuzaki in order to enhance the security of the system by encrypting data and personal identification information by use of an encryption key made out of a given piece of personal identification information, thereby making it difficult to re-create the encryption key by someone having no knowledge of the personal identification information.

Claim 2

Appellant argues that the cited passages of Matsuzaki fail to teach or suggest encrypting the read key information by use of a different encryption key.

Examiner would point out that, Matsuzaki teaches the encryption circuit encrypts the encryption key by use of a different encryption key, and the recording medium records the encryption key encrypted by use of the different encryption key [paragraphs 0148- 0152].

Claim 5

Appellant argues that the cited passages of Matsuzaki do not teach encrypting personal identification information by use of encryption key created out of a given piece of personal identification information. Appellant further argues that, neither Matsuzaki nor Johnson teach encrypting personal identification information by use of a second encryption key created out of a given piece of the person identification information.

Examiner would point out that, in the present application, the term 'personal identification information' is referred as " ... personal identification information by use of an encryption key

created out of a given piece of the personal identification information such as a password ..." [specification page 9, lines 7-10], therefore it is understood by the examiner that, personal identification information is equivalent to a password. The personal identification information in Matsuzaki and Johnson is directed to a password and/or personal ID. Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65].

Claim 6

Appellant argues that, the rejection of claim 6 is in error for at least the reason as claim 5.

Examiner would point out that arguments with respect to claim 5 have be traversed as indicted above and therefore arguments with respect to claim 6 are traversed with the same rationale thereto.

Claim 13

Appellant argues that, the cited portion of Matsuzaki fail to teach encrypting personal identification information and using a piece of the personal identification information as an encryption key. Appellant further argues that, Johnson do not disclose encrypting personal identification information and creating a verification information.

Examiner would point out that, in the present application, the term 'personal identification information' is referred as " ... personal identification information by use of an encryption key

created out of a given piece of the personal identification information such as a password ..." [specification page 9, lines 7-10], therefore it is understood by the examiner that, personal identification information is equivalent to a password. The personal identification information in Matsuzaki and Johnson is directed to a password and/or personal ID. Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65].

Appellant further argues that the Office action has not explained, and it is not evident, how employing the teachings of Johsnon within the system of Matsuzaki enhances the security of the system.

Examiner would point out that a suggestion, teaching, or motivation to combine the relevant prior art teachings does not have to be found explicitly in the prior art, as the teachings, motivation, or suggestion may be implicit from the prior art, as a whole, rather than expressly stated in the references. The test for an implicit showing is what the combined teachings, knowledge of one of a whole would have suggested to those of ordinary skill in the art. In re Kahn, 441 F.3d 977, 988, 78, USPQ2d 1329, 1336 (Fed. Cir. 2006) citing In re Kotzab, 217 F.3d 1365,1370, 55 USPQ2d 1313 (Fed. Cir. 2000). See also In re Thrift, 298 F. 3d 1357, 1363, 63 USPQ2d 2002, 2008 (Fed. Cir. 2002). These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). In this case both Matsuzaki and Johnson are directed a security system, specifically encryption of data/key information using a

password. Matsuzaki teaches encrypting desired data personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. One of ordinary skill in the art at the time of applicant's invention could have been able to employ encryption key creation out of a given piece of personal identification as taught by Johnson and employ it within the system of Matsuzaki in order to enhance the security of the system by encrypting data and personal identification information by use of an encryption key made out of a given piece of personal identification information, thereby making it difficult to re-create the encryption key by someone having no knowledge of the personal identification information.

Claim 14

Appellant argues that, Matsuzaki does not teach or suggest that the file key and the read key are mutually identical.

Examiner would point out that, Matsuzaki teaches the data encryption key and the verification encryption key are mutually identical [paragraphs 0145 & 0150].

Claims 15 and 16

Appellant argues that, the rejection of claim 13 believed to be in error and since claims 15 and 16 depend form claim 13, the rejection of claims 15 and 16 is believed to be in error for at least the same reason as claim 13.

Examiner would point out that arguments with respect to claim 13 have be traversed as indicted above and therefore arguments with respect to claims 15 and 16 are traversed with the same rationale thereto.

Claims 17 and 22

Appellant argues that, the cited portion of Matsuzaki fail to teach encrypting personal identification information and using a piece of the personal identification information as an encryption key. Appellant further argues that, Johnson do not disclose encrypting personal identification information and creating a verification information.

Examiner would point out that, in the present application, the term 'personal identification information' is referred as " ... personal identification information by use of an encryption key created out of a given piece of the personal identification information such as a password ..." [specification page 9, lines 7-10], therefore it is understood by the examiner that, personal identification information is equivalent to a password. The personal identification information in Matsuzaki and Johnson is directed to a password and/or personal ID. Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65].

Appellant further argues that the Office action has not explained, and it is not evident, how employing the teachings of Johsnon within the system of Matsuzaki enhances the security of the system.

Examiner would point out that a suggestion, teaching, or motivation to combine the relevant prior art teachings does not have to be found explicitly in the prior art, as the teachings, motivation, or suggestion may be implicit from the prior art, as a whole, rather than expressly stated in the references. The test for an implicit showing is what the combined teachings, knowledge of one of a whole would have suggested to those of ordinary skill in the art. In re Kahn, 441 F.3d 977, 988, 78, USPQ2d 1329, 1336 (Fed. Cir. 2006) citing In re Kotzab, 217 F.3d 1365,1370, 55 USPQ2d 1313 (Fed. Cir. 2000). See also In re Thrift, 298 F. 3d 1357, 1363, 63 USPQ2d 2002, 2008 (Fed. Cir. 2002). These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). In this case both Matsuzaki and Johnson are directed a security system, specifically encryption of data/key information using a password. Matsuzaki teaches encrypting desired data personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. One of ordinary skill in the art at the time of applicant's invention could have been able to employ encryption key creation out of a given piece of personal identification as taught by Johnson and employ it within the system of Matsuzaki in order to enhance the security of the system by encrypting data and personal identification information by use of an encryption key made out of a given piece of personal identification information, thereby making it difficult to re-create the encryption key by someone having no knowledge of the personal identification information.

Claim 18

Appellant argues that the cited passage of Matsuzaki fail to teach or suggest encrypting the read key information by use of a different encryption key.

Examiner would point out that Matsuzaki teaches encrypting the encryption key by use of a different encryption key and thereby recording the encrypted encryption key in the recording medium [paragraphs 0148-0152].

Claims 19 and 23

Appellant argues that, the cited portion of Matsuzaki fail to teach encrypting personal identification information and using a piece of the personal identification information as an encryption key. Appellant further argues that, Johnson do not disclose encrypting personal identification information and creating a verification information.

Examiner would point out that, in the present application, the term 'personal identification information' is referred as " ... personal identification information by use of an encryption key created out of a given piece of the personal identification information such as a password ..." [specification page 9, lines 7-10], therefore it is understood by the examiner that, personal identification information is equivalent to a password. The personal identification information in Matsuzaki and Johnson is directed to a password and/or personal ID. Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65].

Appellant further argues that the Office action has not explained, and it is not evident, how employing the teachings of Johsnon within the system of Matsuzaki enhances the security of the system.

Examiner would point out that a suggestion, teaching, or motivation to combine the relevant prior art teachings does not have to be found explicitly in the prior art, as the teachings, motivation, or suggestion may be implicit from the prior art, as a whole, rather than expressly stated in the references. The test for an implicit showing is what the combined teachings, knowledge of one of a whole would have suggested to those of ordinary skill in the art. In re Kahn, 441 F.3d 977, 988, 78, USPQ2d 1329, 1336 (Fed. Cir. 2006) citing In re Kotzab, 217 F.3d 1365,1370, 55 USPQ2d 1313 (Fed. Cir. 2000). See also In re Thrift, 298 F. 3d 1357, 1363, 63 USPQ2d 2002, 2008 (Fed. Cir. 2002). These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). In this case both Matsuzaki and Johnson are directed a security system, specifically encryption of data/key information using a password. Matsuzaki teaches encrypting desired data personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Matsuzaki is silent on the device wherein the encryption key is created out of a given piece of the personal identification information. Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. One of ordinary skill in the art at the time of applicant's invention could have been able to employ encryption key creation out of a given piece of personal identification as taught by Johnson and employ it within the system of Matsuzaki in order to enhance the security of the system by encrypting data and personal identification information by use of an encryption key made out of a given piece of personal identification information, thereby making

it difficult to re-create the encryption key by someone having no knowledge of the personal identification information.

Claim 20

Appellant argues that the cited passages of Matsuzaki do not teach encrypting the data encryption key by use of the verification encryption key created out of the personal identification information after the change as required by claim 20.

Examiner would point out that, Matsuzaki teaches encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65].

Claim 21

Appellant argues that the cited passages fail to teach a decrypted encryption key in a recording medium as is required by claim 21.

Examiner would point out that, Matsuzaki teaches decrypting the encrypted data encryption key recorded in the recording medium upon disabling encryption of the data recorded in the recording medium by use of the verification encryption key [paragraphs 0192-0199].

Claim 25

Appellant argues that the cited paragraph of Matsuzaki and Johnson fail to teach encrypting candidate personal identification information and creating a candidate encryption key out of a piece of the candidate personal identification information.

Examiner would point out that, Matsuzaki teaches executing user verification by use of the encrypted personal identification information stored in the recording medium (i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]). Further Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65].

Claim 3

Appellant argues that, Claim 3 is not obvious over Matsuzaki in view of Johnson and further in view of Hirota. Appellant further argues that, the cited portions of Hirota do not discloses the recording medium includes a special storage area which is inaccessible in normal use and the recording medium records the encryption key in the special storage area.

Examiner would point out that, Hirota teaches a recording medium includes a special storage area which is inaccessible in normal use, and the recording medium records the encryption key in the special storage area [see for example, column 12, lines 49-54 and column 10, lines 22-36].

Claim 4

Appellant argues that, Claim 4 is not obvious over Matsuzaki in view of Johnson and further in view of Jackson. Appellant further argues that, the cited portions of Jackson fail to teach a plurality of encryption key which is created out of a plurality of personal identification information as required by claim 4.

Examiner would point out that, Jackson teaches a device wherein the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys [page 8, lines 33-47]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Jackson within the combination of Matsuzaki and Johnson in order to efficiently process encryption/decryption of data.

Claim 7

Appellant argues that Jackson and Johnson do not disclose encrypting personal identification information and creating an encryption key out of a piece of the personal identification information.

Examiner would point out that, Jackson teaches control mechanism executes encryption of the data to be written in the magnetic disk for each unit of writing and reading data in and out of a storage area of the magnetic disk upon processing of writing the data in the magnetic disk [column 11, paragraphs 0041 & 0042], in response to turning on and off of the encryption mechanism (i.e., activating the encryption/decryption only in response to receipt of a valid password) [column 5, lines 19-34], wherein the encryption function of the control mechanism encrypts personal identification information by use of an encryption key [page 7, paragraph 0028 and page 8, lines 21-32]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65].

Claim 8

Appellant argues that the cited portions of Jackson fails to teach judging as to whether data are encrypted or not as is required by claim 8.

Examiner would point out that, , Jackson teaches the device wherein the control mechanism judges as to whether the data are encrypted or not upon reading the data out of the storage medium, and further decrypts the data when the data are encrypted [page 11, paragraphs 0041-0042].

Claims 9 and 10

Appellant argues that claim 9 and 10 depend from claim 7 and are believed to be in error for at lest the same reason as claim 7.

Examiner would point out that arguments with respect to claim 7 have be traversed as indicted above and therefore arguments with respect to claims 9 and 10 are traversed with the same rationale thereto.

Claim 11

Appellant argues that, the cited passage of Jackson fails to teach a plurality of encryption keys which is created out of a plurality of personal identification information as required by claim 11 and further fails to teach controlling user identification depending on each of the plurality of encryption keys.

Examiner would point out that, Jackson teaches encrypting personal identification information by use of an encryption key [page 7, paragraph 0028 and page 8, lines 21-32]. Further, Johnson teaches a personal authentication device, including creating a plurality of

encryption keys out of a given piece of personal identification information [column 10, lines 48-65].

Claim 12

Appellant argues that claim 12 depend from claim 7 and are believed to be in error for at lest the same reason as claim 7.

Examiner would point out that arguments with respect to claim 7 have be traversed as indicted above and therefore arguments with respect to claim 12 are traversed with the same rationale thereto.

Claim 24

Appellant argues that, Jackson fails to teach writing data in the recording medium without encrypting the data when the encryption function is turned off.

Examiner would point out that, Jackson teaches writing the data in the recording medium without encrypting the data when the encryption function is turned off [column 5, lines 19-34].

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Beemnet W Dada/

Conferees:

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135

/Hosuk Song/

Primary Examiner, Art Unit 2135